CLAIMS

1. A method for broadcast encryption, comprising:

assigning each user in a group of users respective private information I_u;

selecting at least one session encryption key K;

partitioning users not in a revoked set R into disjoint subsets S_{i1},...S_{im} having associated subset keys L_{i1},...L_{im}; and

encrypting the session key K with the subset keys L_{i1},...,L_{im} to render m encrypted versions of the session key K.

2. The method of Claim 1, further comprising partitioning the users into groups S_1,...,S_w, wherein "w" is an integer, and the groups establish subtrees in a tree.

3. The method of Claim 2, wherein the tree is a complete binary tree.

4. The method of Claim 1, further comprising using private information I_u to decrypt the session key.

5. The method of Claim 4, wherein the act of decrypting includes using information i_j such that a user belongs to a subset S_{ij}, and retrieving a subset key L_{ij} using the private information of the user.

6. The method of Claim 2, wherein each subset S_{i1},...S_{im} includes all leaves in a subtree rooted at some node v_i, at least each node in the subtree being associated with a respective subset key.

7. The method of Claim 6, wherein content is provided to users in at least one message defining a header, and the header includes at most r*log(N/r) subset keys and encryptions, wherein r is the number of users in the revoked set R and N is the total number of users.

8. The method of Claim 6, wherein each user must store log N keys, wherein N is the total number of users.

9. The method of Claim 6, wherein content is provided to users in at least one message, and wherein each user processes the message using at most log log N operations plus a single decryption operation, wherein N is the total number of users.

10. The method of Claim 6, wherein the revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

11. The method of Claim 2, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i.

12. The method of Claim 11, wherein content is provided to users in at least one message defining a header, and the header includes at most 2r-1 subset keys and encryptions, wherein r is the number of users in the revoked set R.

13. The method of Claim 11, wherein each user must store .5log^2 N + .5log N +1 keys, wherein N is the total number of users.

14. The method of Claim 11, wherein content is provided to users in at least one message, and wherein each user processes the message using at most log N operations plus a single decryption operation, wherein N is the total number of users.

15. The method of Claim 11, wherein the revoked set R defines a spanning tree, and wherein the method includes:

initializing a cover tree T as the spanning tree;

iteratively removing nodes from the cover tree T and adding nodes to a cover until the cover tree T has at most one node.

16. The method of Claim 11, wherein each node has at least one label possibly induced by at least one of its ancestors, and wherein each user is assigned labels from all nodes hanging from a direct path between the user and the root but not from nodes in the direct path.

17. The method of Claim 16, wherein labels are assigned to subsets using a pseudorandom sequence generator, and the act of decrypting includes evaluating the pseudorandom sequence generator.

18. The method of Claim 1, wherein content is provided to users in at least one message having a header including a cryptographic function E_L, and the method includes prefix-truncating the cryptographic function E_L.

19. The method of Claim 2, wherein the tree includes a root and plural nodes, each node having an associated key, and wherein each user is assigned keys from all nodes in a direct path between a leaf representing the user and the root.

20. The method of Claim 1, wherein content is provided to users in at least one message defining plural portions, and each portion is encrypted with a respective session key.

21. A computer program device, comprising:

a computer program storage device including a program of instructions usable by a computer, comprising:

logic means for accessing a tree to identify plural subset keys;

logic means for encrypting a message with a session key;

logic means for encrypting the session key at least once with each of the subset keys to render encrypted versions of the session key; and logic means for sending the encrypted versions of the session key in a header of the message to plural stateless receivers.

22. The computer program device of Claim 21, further comprising:

logic means for partitioning receivers not in a revoked set R into disjoint subsets S_{i1},...S_{im} having associated subset keys L_{i1},...,L_{im}.

23. The computer program device of Claim 22, further comprising logic means for partitioning the users into groups S_1,...,S_w, wherein "w" is an integer, and the groups establish subtrees in a tree.

24. The computer program device of Claim 21, further comprising logic means for using private information I_u to decrypt the session key.

25. The computer program device of Claim 24, wherein the means for decrypting includes logic means for using information i_j such that a receiver belongs to a subset S_{ij}, and retrieving a key L_{ij} from the private information of the receiver.

26. The computer program device of Claim 23, wherein each subset S_{i1},...S_{im} includes all leaves in a subtree rooted at some node v_i, at least each node in the subtree being associated with a respective subset key.

27. The computer program device of Claim 26, wherein logic means provide content to receivers in at least one message defining a header, and the header includes at most r*log(N/r) subset keys and encryptions, wherein r is the number of receivers in the revoked set R and N is the total number of receivers.

28. The computer program device of Claim 26, wherein each receiver must store log N keys, wherein N is the total number of receivers.

29. The computer program device of Claim 26, wherein logic means provide content to receivers in at least one message, and wherein each receiver processes the message using at most log log N operations plus a single decryption operation, wherein N is the total number of receivers.

30. The computer program device of Claim 26, wherein the revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

31. The computer program device of Claim 23, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i.

32. The computer program device of Claim 31, wherein logic means provide content to receivers in at least one message defining a header, and the header includes at most 2r-1 subset keys and encryptions, wherein r is the number of receivers in the revoked set R.

33. The computer program device of Claim 31, wherein each receiver must store .5log^2 N + .5log N +1 keys, wherein N is the total number of receivers.

34. The computer program device of Claim 31, wherein logic means provide content to receivers in at least one message, and wherein each receiver processes the message using at most log N operations plus a single decryption operation, wherein N is the total number of receivers.

35. The computer program device of Claim 31, wherein the revoked set R defines a spanning tree, and wherein the computer program device includes:

logic means for initializing a cover tree T as the spanning tree; and

logic means for iteratively removing nodes from the cover tree T and adding nodes to a cover until the cover tree T has at most one node.

36. The computer program device of Claim 35, wherein logic means assign labels to receivers using a pseudorandom sequence generator, and the labels induce subset keys.

37. The computer program device of Claim 36, wherein the means for decrypting includes evaluating the pseudorandom sequence generator.

38. The computer program device of Claim 21, wherein logic means provide content to receivers in at least one message having a header including a cryptographic function E_L, and the computer program device includes logic means for prefix-truncating the cryptographic function E_L.

39. The computer program device of Claim 23, wherein the tree includes a root and plural nodes, each node having an associated key, and wherein logic means assign each receiver keys from all nodes in a direct path between a leaf representing the receiver and the root.

40. The computer program device of Claim 21, wherein logic means provide content to receivers in at least one message defining plural portions, and each portion is encrypted with a respective session key.

41. A computer programmed with instructions to cause the computer to execute method acts including:

encrypting broadcast content; and

sending the broadcast content to plural stateless good receivers and to at least one revoked receiver such that each stateless good receiver can decrypt the content and the revoked receiver cannot decrypt the content.

42. The computer of Claim 41, wherein the method acts further comprise:

assigning each receiver in a group of receivers respective private information I_u;

selecting at least one session encryption key K;

partitioning all receivers not in a revoked set R into disjoint subsets $S_{i1},...S_{im}$ having associated subset keys $L_{i1},...,L_{im}$; and

encrypting the session key K with the subset keys $L_{i1},...,L_{im}$ to render m encrypted versions of the session key K.

43. The computer of Claim 41, wherein the method acts undertaken by the computer further comprise partitioning the users into groups $S_1,...,S_w$, wherein "w" is an integer, and the groups establish subtrees in a tree.

44. The computer of Claim 43, wherein the tree is a complete binary tree.

44. The computer of Claim 41, wherein the method acts include using private information I_u to decrypt the session key.

45. The computer of Claim 44, wherein the act of decrypting undertaken by the computer includes using information i_j such that a receiver belongs to a subset S_{ij}, and retrieving a key L_{ij} using the private information of the receiver.

46. The computer of Claim 43, wherein each subset $S_{i1},...S_{im}$ includes all leaves in a subtree rooted at some node v_i, at least each node in the subtree being associated with a respective subset key.

47. The computer of Claim 46, wherein content is provided to receivers in at least one message defining a header, and the header includes at most r*log(N/r) subset keys and encryptions, wherein r is the number of receivers in the revoked set R and N is the total number of receivers.

48. The computer of Claim 46, wherein each receiver must store log N keys, wherein N is the total number of receivers.

49. The computer of Claim 46, wherein content is provided to receivers in at least one message, and wherein each receiver processes the message using at most log log N operations plus a single decryption operation, wherein N is the total number of receivers.

50. The computer of Claim 46, wherein the revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

51. The computer of Claim 43, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i.

52. The computer of Claim 51, wherein content is provided to receivers in at least one message defining a header, and the header includes at most 2r-1 subset keys and encryptions, wherein r is the number of receivers in the revoked set R.

53. The computer of Claim 51, wherein each receiver must store .5log^2 N + .5log N +1 keys, wherein N is the total number of receivers.

54. The computer of Claim 51, wherein content is provided to receivers in at least one message, and wherein each receiver processes the message using at most log N operations plus a single decryption operation, wherein N is the total number of receivers.

55. The computer of Claim 51, wherein the revoked set R defines a spanning tree, and wherein the method acts undertaken by the computer further include:

initializing a cover tree T as the spanning tree;

iteratively removing nodes from the cover tree T and adding nodes to a cover until the cover tree T has at most one node.

56. The computer of Claim 55, wherein the computer assigns node labels to receivers from the tree using a pseudorandom sequence generator.

57. The computer of Claim 56, wherein the act of decrypting undertaken by the computer includes evaluating the pseudorandom sequence generator.

58. The computer of Claim 41, wherein content is provided to receivers in at least one message having a header including a cryptographic function E_L, and the method acts undertaken by the computer include prefix-truncating the cryptographic function E_L.

59. The computer of Claim 41, wherein content is provided to receivers in at least one message defining plural portions, and each portion is encrypted by the computer with a respective session key.

60. The method of Claim 11, wherein each node has plural labels with each ancestor of the node inducing a respective label, and wherein each user is assigned labels from all nodes hanging from a direct path between the user and the root but not from nodes in the direct path.

61. A method for broadcast encryption, comprising:

assigning each user in a group of users respective private information I_u;

selecting at least one session encryption key K;

partitioning all users into groups S_1,...,S_w, wherein "w" is an integer, and the groups establish subtrees in a tree;

partitioning users not in a revoked set R into disjoint subsets S_{i1},...S_{im} having associated subset keys L_{i1},...L_{im}; and

encrypting the session key K with the subset keys L_{i1},...,L_{im} to render m encrypted versions of the session key K, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i.

62. A potentially stateless receiver in a multicast system, comprising:

at least one data storage device storing plural labels of nodes that are not in a direct path between the receiver and a root of a tree having a leaf representing the receiver, but that hang off the direct path and that are induced by some node v_i, an ancestor of the leaf representing the receiver, the labels establishing private information I_u of the receiver usable by the receiver to decrypt subset keys derived from the labels.

63. The receiver of Claim 62, wherein the receiver computes the subset keys of all sets except a direct path set that are rooted at the node v_i by evaluating a pseudorandom function, but can compute no other subset keys.

64. The receiver of Claim 62, wherein the receiver decrypts a session key using at least one subset key, the session key being useful for decrypting content.

65. A receiver of content, comprising:

means for storing respective private information I_u;

means for receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content; and means for obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content.

66. The receiver of Claim 65, wherein the receiver is partitioned into one of a set of groups $S_1,\ldots,S_w$, wherein "w" is an integer, and the groups establish subtrees in a tree defining nodes and leaves.

67. The receiver of Claim 66, wherein subsets $S_{i1},\ldots,S_{im}$ derived from the set of groups $S_1,\ldots,S_w$ define a cover.

68. The receiver of Claim 67, wherein the receiver receives content in at least one message defining a header, and the header includes at most r*log(N/r) subset keys and encryptions, wherein r is the number of receivers in a revoked set R and N is the total number of receivers.

69. The receiver of Claim 67, wherein the receiver must store log N keys, wherein N is the total number of receivers.

70. The receiver of Claim 67, wherein the receiver receives content in at least one message defining a header, and wherein the receiver processes the message using at most log log N operations plus a single decryption operation, wherein N is the total number of receivers.

71. The receiver of Claim 67, wherein a revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

72. The receiver of Claim 67, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i.

73. The receiver of Claim 72, wherein the receiver receives content in a message having a header including at most 2r-1 subset keys and encryptions, wherein r is the number of receivers in the revoked set R.

74. The receiver of Claim 72, wherein the receiver must store $.5\log^2 N + .5\log N +1$ keys, wherein N is the total number of receivers.

75. The receiver of Claim 72, wherein content is provided to the receiver in at least one message, and wherein the receiver processes the message using at most log N operations plus a single decryption operation, wherein N is the total number of receivers.

76. The receiver of Claim 72, wherein the receiver decrypts the subset key by evaluating a pseudorandom sequence generator.

77. A receiver of content, comprising:

a data storage storing respective private information I_u;

a processing device receiving at least one session encryption key K encrypted with plural subset keys, the session key encrypting content, the processing device obtaining at least one subset key using the private information such that the session key K can be decrypted to play the content.

78. The receiver of Claim 77, wherein the receiver is partitioned into one of a set of groups $S_1,\ldots,S_w$, wherein "w" is an integer, and the groups establish subtrees in a tree.

79. The receiver of Claim 78, wherein subsets $S_{i1},\ldots,S_{im}$ derived from the set of groups $S_1,\ldots,S_w$ define a cover.

80. The receiver of Claim 79, wherein the receiver receives content in at least one message defining a header, and the header includes at most r*log(N/r) subset keys and encryptions, wherein r is the number of receivers in a revoked set R and N is the total number of receivers.

81. The receiver of Claim 79, wherein the receiver must store log N keys, wherein N is the total number of receivers.

82. The receiver of Claim 79, wherein the receiver receives content in at least one message defining a header, and wherein the receiver processes the message using at most log log N operations plus a single decryption operation, wherein N is the total number of receivers.

83. The receiver of Claim 79, wherein one revoked set R defines a spanning tree, and subtrees having roots attached to nodes of the spanning tree define the subsets.

84. The receiver of Claim 79, wherein the tree includes a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i.

85. The receiver of Claim 84, wherein the receiver receives content in a message having a header including at most 2r-1 subset keys and encryptions, wherein r is the number of receivers in the revoked set R.

86. The receiver of Claim 84, wherein the receiver must store $.5\log^2 N + .5\log N + 1$ keys, wherein N is the total number of receivers.

87. The receiver of Claim 84, wherein content is provided to the receiver in at least one message, and wherein the receiver processes the message using at most log N operations plus a single decryption operation, wherein N is the total number of receivers.

88. The receiver of Claim 84, wherein the receiver decrypts the subset key by evaluating a pseudorandom sequence generator.

89. A medium holding a message of content of the general form $\mathbf{<[i_1, i_2,\ldots,i_m, E_{Li1}(K), E_{Li2}(K),\ldots,E_{Lim}(K)], F_K(M)>}$, wherein K is a session key, F_K is an encryption primitive, E_K is an encryption primitive, L_i are subset keys associated with subsets of receivers in an encryption broadcast system, M is a message body, and $i_1, i_2,\ldots,i_m$ are tree node subsets defining a cover.

90. The medium of Claim 89, wherein the encryption primitive F_K is implemented by XORing the message body M with a stream cipher generated by the session key K.

91. The medium of Claim 89, wherein E_L is a Prefix-Truncation specification of a block cipher, ⊗ represents a random string whose length equals the block length of E_L, and K is a short key for F_K, and the message is of the form

$$\mathbf{<[i_1, i_2,\ldots,i_m, U, [\text{Prefix}_{|K|} E_{Li1}(U)] \oplus K,\ldots,[\text{Prefix}_{|K|} E_{Lim}(U)] \oplus K], F_K(M)>}.$$

92. The medium of Claim 91, wherein $\otimes \oplus i_j$ is encrypted and the message is of the form

$$\mathbf{<[i_1, i_2,\ldots,i_m, U, [\text{Prefix}_{|L|} E_{Li1}(U \oplus i_1)] \oplus K,\ldots,[\text{Prefix}_{|L|} E_{Lim}(U \oplus i_m)] \oplus K], F_K(M)>}.$$

93. The medium of Claim 89, wherein the subset keys are derived from a tree including a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i that are not in the subtree rooted at some other node v_j that descends from v_i.

94. The medium of Claim 89, wherein the subset keys are derived from a tree including a root and plural nodes, each node having at least one associated label, and wherein each subset includes all leaves in a subtree rooted at some node v_i, at least each node in the subtree being associated with a respective subset key.

95. The computer of Claim 42, wherein the act of partitioning is undertaken by a system computer in a system of receivers separate from the system computer.

96. The computer of Claim 42, wherein the act of partitioning is undertaken by a receiver computer.

97. The receiver of Claim 67, wherein the receiver derives the subsets in the cover.